AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A method of encrypting an object, comprising the steps of

a first active agent initiating the first key management component generating a first key management component public key/first key management component private key pair;

loading an object encryption component;

loading an object decryption component;

creating a correlation table;

a second active agent transmitting an encrypt object request to the first key management component;

the first key management component transmitting an object encryption component to the second active agent computing platform over a secure channel;

the first key management component transmitting the first key management component public key to the second active agent computing platform over a secure channel;

the object encryption component generating a symmetric key;

the object encryption component encrypting a clear text object with the symmetric key;

the object encryption component encrypting the symmetric key with the first key management component public key;

the object encryption component creating an association between the encrypted symmetric key and the cipher text object

the object encryption component transmitting the encrypted symmetric key to the first key management component or to a second key management component having the first key management component private key;

the object encryption component transmitting the association to the key management component having received the encrypted symmetric key; and,

the key management component having received the association entering the association into the correlation table.

2. (Original) The method of claim 1, further comprising the step of the object encryption component transmitting the cipher text object to a computing platform.

3. (Original) The method of claim 1, wherein the first key management component public key/first key management component private key pair is generated using an encryption algorithm selected from the group consisting of ECC and RSA.

4. (Original) The method of claim 1, wherein the secure channel is an SSL channel.

5. (Original) The method of claim 1, wherein the object encryption component is installed on a browser.

6. (Original) The method of claim 5, wherein the browser is the Internet Explorer™ or the Navigator®.

7. (Original) The method of claim 5, wherein the object encryption component is implemented as a Java® applet.

8. (Original) The method of claim 5, wherein the browser is the Internet Explorer™ and the object encryption component is implemented as an Active X™ control.

9. (Original) The method of claim 1, wherein the object encryption component is comprised of a symmetric encryption algorithm selected from the group consisting of IDEA, DES, Blowfish, RC4, RC2, SAFER, and AES.

10. (Original) A method of decrypting an object, comprising the steps of:

an active agent transmitting a decrypt object request to the key management component;

the key management component retrieving a cipher text object symmetric key from a correlation table;

the key management component decrypting cipher text object symmetric key with the key management component private key;

the key management component transmitting the object decryption component to the active agent computing platform over a secure channel;

the key management component transmitting the cipher text object symmetric key to the active agent computing platform over a secure channel; and

the object decryption component decrypting the cipher text object with the cipher text object symmetric key.

11. (Original) The method of claim 10, further comprising the step of the active agent transmitting the cipher text object request to a computing platform.

12. (Original) The method of claim 10, further comprising the step of a computer platform transmitting the cipher text object to the active agent computing platform.

13. (Original) The method of claim 10, wherein the secure channel is an SSL channel.

14. (Original) The method of claim 10, wherein the object decryption component is installed on a browser.

15. (Original) The method of claim 14, wherein the browser is the Internet Explorer™ or the Navigator®.

16. (Original) The method of claim 14, wherein the object decryption component is implemented as a Java® applet.

17. (Original) The method of claim 14, wherein the browser is the Internet Explorer™ and the object encryption component is implemented as an Active X™ control.

18. (Original) The method of claim 10, wherein the object decryption component is comprised of a symmetric encryption algorithm selected from the group consisting of IDEA, DES, Blowfish, RC4, RC2, SAFER, and AES.

19. (Original) A method of encrypting an object, comprising:

under control of a first encryption server system, generating a public/private key pair for an encryption server system;

under control of a client system, requesting an encryption program from an encryption server system;

requesting a server public key from an encryption server system;

under the control of an encryption server system, transmitting an encryption program to a client system over a secure channel;

transmitting a server public key to a client system over a secure channel;

under control of a client system, receiving an encryption program from an encryption server system over a secure channel;

receiving a server public key from an encryption server system over a secure channel;

installing an encryption program on a client system;

running an encryption program on a client system to generate a symmetric key;

encrypting a clear text object with a symmetric key, thereby creating a cipher text object;

creating a relationship between a cipher text object and a symmetric key;

encrypting symmetric key with an encryption server public key, thereby creating an encrypted symmetric key;

creating a relationship between a cipher text object and an encrypted symmetric key;

transmitting a cipher text object to an encryption server system;

transmitting an encrypted symmetric key to an encryption server system;

transmitting the relationship between a cipher text object and an encrypted symmetric key to an encryption server system;

under the control of an encryption server system,

storing a cipher text object in a storage medium;

storing an encrypted symmetric key in a storage medium; and

storing the relationship between a cipher text object and an encrypted symmetric key in a storage medium.

20. (Original) An encryption system for transparent key management object encryption, comprising:

an encryption server system and a client system;

an encryption server system, generating a public/private key pair for an encryption server system;

transmitting an encryption program to a client system over a secure channel;

transmitting a server public key to a client system over a secure channel;

storing an encrypted object in a storage medium;

storing an encrypted symmetric key in a storage medium;

storing the relationship created between a object and a symmetric key in a storage medium;

a client system, requesting an encryption program from an encryption server system;

requesting a server public key from an encryption server system;

receiving an encryption program from encryption server system over a secure channel;

receiving a server public key from encryption server system over a secure channel;

installing an encryption program on a client system;

running an encryption program on a client system to generate a symmetric key;

encrypting a clear text object with a symmetric key, thereby creating a cipher text object;

creating a relationship between a cipher text object and a symmetric key;

encrypting symmetric key with an encryption server public key,

thereby creating an encrypted symmetric key;

creating a relationship between a cipher text object and a encrypted symmetric key;

transmitting a cipher text object to an encryption server system;

transmitting an encrypted symmetric key to an encryption server system;

transmitting the relationship between a cipher text object and an encrypted symmetric key to an encryption server system.

21. (Original) An encryption system for transparent key management object encryption, comprising:

an encryption server system and a client system;

an encryption server system,

using the first entry in a correlation table to retrieve an encrypted symmetric key;

decrypting a symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key;

inserting a symmetric key into a decryption program;

sending a decryption program to a client system over a secure channel;

sending a cipher text object to a client system;

under control of a client system, requesting a cipher text object from a server;

under control of an encryption server system, installing a decryption program on a client system; and,

decrypting a cipher text object using a decryption program, thereby creating a clear text object.

22. (Original) An encryption system for transparent key management object encryption, comprising:

an encryption server system and a client system;

under control of an encryption server system,

generating a symmetric key;

encrypting a clear text object with a symmetric key, thereby creating a cipher text object;

inserting a symmetric key into a decryption program;

sending a decryption program to a client system over a secure channel;

sending a cipher text object to a client system;

under control of a client system,

requesting a clear text object from a server;

installing a decryption program on a client system; and,

decrypting a cipher text object using a decryption program, thereby creating a clear text object.

23. (Original) An encryption system for transparent key management object encryption, comprising:

an encryption server system and a client system;

an encryption server system,

generating a public/private key pair for an encryption server system;

transmitting an encryption program to a client system over a secure channel;

transmitting a server public key to a client system over a secure channel;

storing a cipher text object in a storage medium;

storing an encrypted symmetric key in a storage medium;

storing the relationship created between a cipher text object and an encrypted symmetric key in a storage medium;

using the first entry in a correlation table to retrieve an encrypted symmetric key;

decrypting a symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key;

inserting an encrypted symmetric key into a decryption program;

sending a decryption program to a client system over a secure channel;

sending a cipher text object to a client system;

decrypting an encrypted symmetric key using an encryption server system private key, thereby creating a decrypted symmetric key;

sending a cipher text object to a client system;

generating a symmetric key; encrypting a clear text object with a symmetric key, thereby creating a cipher text object;

a client system, requesting an encryption program from an encryption server system;

requesting a server public key from an encryption server system;

receiving an encryption program from encryption server system over a secure connection;

receiving a server public key from an encryption server system over a secure channel;

installing an encryption program on a client system;

running an encryption program on a client system to generate a symmetric key;

encrypting a clear text object with a symmetric key, thereby creating a cipher text object;

creating a relationship between a cipher text object and a symmetric key;

encrypting symmetric key with an encryption server public key, thereby creating an encrypted symmetric key;

creating a relationship between a cipher text object and an encrypted symmetric key;

transmitting an object encrypted with a symmetric key from a client system to an encryption server system;

transmitting a symmetric key encrypted with a server public key from a client system to a encryption server system;

transmitting the relationship between a cipher text object and an encrypted symmetric key to an encryption server system;

requesting a cipher text object from a server;

installing a decryption program on a client system; and,

decrypting a cipher text object using a decryption program, thereby creating a clear text object; and, requesting a clear text object from a server.